PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

BERGGREN OY AB
P.O. Box 16
FIN-00101 Helsinki
FINLANDE

Date of mailing (day/month/year)
05 décembre 2001 (05.12.01)

Applicant's or agent's file reference
49769

IMPORTANT NOTIFICATION

International application No.
PCT/FI00/00421

International filing date (day/month/year)
11 mai 2000 (11.05.00)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address
NOKIA NETWORKS OY
P.O. Box 300
FIN-00045 Nokia Group
Finland

State of Nationality: FI
State of Residence: FI
Telephone No.: +358-9-51121
Facsimile No.: +358-9-51168080
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [ ] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address
NOKIA CORPORATION
Keilalahdentie 4
FIN-02150 Espoo
Finland

State of Nationality: FI
State of Residence: FI
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

Authorized officer
Marie-José DEVILLARD
Telephone No.: (41-22) 338.83.38

The demand must be filed directly with the competent International Preliminary Examining Authority or, if two or more Authorities are competent, with the one chosen by the applicant. The full name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/ EPO

PCT

CHAPTER II

DEMAND

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only

Identification of IPEA	Date of receipt of DEMAND

Box No. I IDENTIFICATION OF THE INTERNATIONAL APPLICATION		Applicant's or agent's file reference: 49769/ML/JK/MM
International application No.: PCT/FI00/00421	International filing date *(day/month/year)*: 11 May 2000 (11.5.00)	(Earliest) Priority date *(day/month/year)*: 11 May 1999 (11.5.99)

Title of invention:
INTEGRITY PROTECTION METHOD FOR RADIO NETWORK SIGNALING

Box No. II APPLICANT(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

NOKIA NETWORKS OY
P.O. Box 300
FIN-00045 NOKIA GROUP
Finland

Telephone No.:

Facsimile No.:

Teleprinter No.:

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
Finland	Finland

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

NIEMI, Valtteri
Itämerenkatu 11-13
FIN-00180 HELSINKI
Finland

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
Finland	Finland

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

RAJANIEMI, Jaakko
Lapinrinne 2 A 11
FIN-00180 HELSINKI
Finland

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
Finland	Finland

[x] Further applicants are indicated on a continuation sheet.

Sheet No. 2

International application No.
PCT/FI00/00421

Continuation of Box No. II APPLICANT(S)

If none of the following sub-boxes is used, this sheet should not be included in the demand.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

MUHONEN, Ahti
Holperintie 39
FIN-04680 HIRVIVAARA
Finland

State *(that is, country)* of nationality:	State *(that is, country)* of residence:
Finland	Finland

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

State *(that is, country)* of nationality:	State *(that is, country)* of residence:

☐ Further applicants are indicated on another continuation sheet.

International application No.
PCT/FI00/00421

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The following person is [X] agent [ ] common representative

and [X] has been appointed earlier and represents the applicant(s) also for international preliminary examination.

[ ] is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.

[ ] is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

BERGGREN OY AB
P.O. Box 16
FIN-00101 HELSINKI
Finland

Telephone No.: +358-9-693701

Facsimile No.: +358-9-6933944

Teleprinter No.:

[ ] **Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special addr ess to which correspondence should be sent.**

Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION

Statement concerning amendments:*

1. The applicant wishes the international preliminary examination to start on the basis of:

[ ] the international application as originally filed

the description [ ] as originally filed
[ ] as amended under Article 34

the claims [ ] as originally filed
[ ] as amended under Article 19 (together with any accompanying statement)
[ ] as amended under Article 34

the drawings [ ] as originally filed
[ ] as amended under Article 34

2. [ ] The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.

3. [ ] The applicant wishes the start of the international preliminary examination to be postponed until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). *(This check-box may be marked only where the time limit under Article 19 has not yet expired.)*

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: English

[X] which is the language in which the international application was filed.

[ ] which is the language of a translation furnished for the purposes of international search.

[X] which is the language of publication of the international application.

[ ] which is the language of the translation (to be) furnished for the purposes of international preliminary examination.

Box No. V ELECTION OF STATES

The applicant hereby elects all eligible States *(that is, all States which have been designated and which are bound by Chapter II of the PCT)*

excluding the following States which the applicant wishes not to elect:

International application No.
PCT/FI00/00421

Box No. VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:			For International Preliminary Examining Authority use only: received	not received
1. translation of international application	:	sheets	☐	☐
2. amendments under Article 34	:	sheets	☐	☐
3. copy (or, where required, translation) of amendments under Article 19	:	sheets	☐	☐
4. copy (or, where required, translation) of statement under Article 19	:	sheets	☐	☐
5. letter	:	sheets	☐	☐
6. other *(specify)*	:	sheets	☐	☐

The demand is also accompanied by the item(s) marked below:

1. [X] fee calculation sheet
2. [ ] separate signed power of attorney
3. [ ] copy of general power of attorney; reference number, if any:
4. [ ] statement explaining lack of signature
5. [ ] nucleotide and or amino acid sequence listing in computer readable form
6. [ ] other *(specify)*:

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).

BERGGREN OY AB

Juhani Kupiainen
Patent Agent

7 December 2000

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:
2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):
3. ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply. ☐ The applicant has been informed accordingly.
4. ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.
5. ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

CHAPTER II

PCT

FEE CALCULATION SHEET

Annex to the Demand for international preliminary examination

International application No.	PCT/FI00/00421
Applicant's or agent's file reference	49769/ML/JK/MM

For International Preliminary Examining Authority use only

Date stamp of the IPEA

Applicant

NOKIA NETWORKS OY

Calculation of prescribed fees

1. Preliminary examination fee	EUR 1533	P
2. Handling fee *(Applicants from certain States are entitled to a reduction of 75% of the handling fee. Where the applicant is (or all applicants are) so entitled, the amount to be entered at H is 25% of the handling fee.)*	EUR 147	H
3. Total of prescribed fees Add the amounts entered at P and H and enter total in the TOTAL box	EUR 1680	TOTAL

Mode of Payment

☐	authorization to charge deposit account with the IPEA (see below)	☐	cash
☐	cheque	☐	revenue stamps
☐	postal money order	☐	coupons
☒	bank draft	☐	other *(specify)*: Bank transfer to account 157230-340380

Deposit Account Authorization *(this mode of payment may not be available at all IPEAs)*

The IPEA/ EPO ☐ is hereby authorized to charge the total fees indicated above to my deposit account.

☐ *(this check-box may be marked only if the conditions for deposit accounts of the IPEA so permit)* is hereby authorized to charge any deficiency or credit any overpayment in the total fees indicated above to my deposit account.

Deposit Account Number | Date *(day/month/year)* | Signature

See Notes to the fee calculation sheet

PCT REQUEST

Original (for SUBMISSION) - printed on 11.05.2000 09:31:37 AM

10/009658 49769

0 0-1	**For receiving Office use only** International Application No.	
0-2	International Filing Date	
0-3	Name of receiving Office and "PCT International Application"	
0-4 0-4-1	**Form - PCT/RO/101 PCT Request** Prepared using	PCT-EASY Version 2.90 (updated 08.03.2000)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	National Board of Patents and Registration (Finland) (RO/FI)
0-7	**Applicant's or agent's file reference**	49769
I	**Title of invention**	INTEGRITY PROTECTION METHOD FOR RADIO NETWORK SIGNALING
II II-1 II-2 II-4 II-5 II-6 II-7 II-8 II-9	**Applicant** This person is: Applicant for Name Address: State of nationality State of residence Telephone No. Facsimile No.	applicant only all designated States except US NOKIA NETWORKS OY P.O. Box 300 FIN-00045 Nokia Group Finland FI FI +358-9-51121 +358-9-51168080
III-1 III-1-1 III-1-2 III-1-4 III-1-5 III-1-6 III-1-7	**Applicant and/or inventor** This person is: Applicant for Name (LAST, First) Address: State of nationality State of residence	applicant and inventor US only NIEMI, Valtteri Itämerenkatu 11-13 FIN-00180 Helsinki Finland FI FI

PCT REQUEST 49769

Original (for **SUBMISSION**) - printed on 11.05.2000 09:31:37 AM

III-2	**Applicant and/or inventor**	
III-2-1	This person is:	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	RAJANIEMI, Jaakko
III-2-5	Address:	Lapinrinne 2 A 11 FIN-00180 Helsinki Finland
III-2-6	State of nationality	FI
III-2-7	State of residence	FI
III-3	**Applicant and/or inventor**	
III-3-1	This person is:	applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	MUHONEN, Ahti
III-3-5	Address:	Holperintie 39 FIN-04680 Hirvivaara Finland
III-3-6	State of nationality	FI
III-3-7	State of residence	FI
IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name	BERGGREN OY AB
IV-1-2	Address:	P.O. Box 16 FIN-00101 Helsinki Finland
IV-1-3	Telephone No.	+358-9-693701
IV-1-4	Facsimile No.	+358-9-6933944
IV-1-5	e-mail	email.box@berggren.fi
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW SD SL SZ TZ UG ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT

PCT REQUEST

49769

Original (for SUBMISSION) - printed on 11.05.2000 09:31:37 AM

V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AG AL AM AT AU AZ BA BB BG BR BY CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW	
V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.		
V-6	**Exclusion(s) from precautionary designations**	NONE	
VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	11 May 1999 (11.05.1999)	
VI-1-2	Number	991088	
VI-1-3	Country	FI	
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1	
VII-1	**International Searching Authority Chosen**	European Patent Office (EPO) (ISA/EP)	
VIII	**Check list**	number of sheets	electronic file(s) attached
VIII-1	Request	4	-
VIII-2	Description	11	-
VIII-3	Claims	1	-
VIII-4	Abstract	1	49769.txt
VIII-5	Drawings	2	-
VIII-7	TOTAL	19	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-9	Separate signed power of attorney	✓	-
VIII-10	Copy of general power of attorney	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-17	Other (specified):	Copy of Official Action in FI 991088	-
VIII-18	**Figure of the drawings which should accompany the abstract**	1	

PCT REQUEST

49769

Original (for **SUBMISSION**) - printed on 11.05.2000 09:31:37 AM

VIII-19	**Language of filing of the international application**	English
IX-1	**Signature of applicant or agent**	
IX-1-1	Name	BERGGREN OY AB
IX-1-2	Name of signatory	Markus Levlin
IX-1-3	Capacity	Patent Agent

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/EP
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

PCT (ANNEX - FEE CALCULATION SHEET)

49769

Original (for **SUBMISSION**) - printed on 11.05.2000 09:31:37 AM

(This sheet is not part of and does not count as a sheet of the international application)

0 0-1	**For receiving Office use only** International Application No.				
0-2	Date stamp of the receiving Office				
0-4 0-4-1	**Form - PCT/RO/101 (Annex)** **PCT Fee Calculation Sheet** Prepared using		PCT-EASY Version 2.90 (updated 08.03.2000)		
0-9	**Applicant's or agent's file reference**		49769		
2	**Applicant**		NOKIA NETWORKS OY, et al.		
12	**Calculation of prescribed fees**		fee amount/multiplier	total amounts (FIM)	
12-1	Transmittal fee	T	⇨	800	
12-2	Search fee	S	⇨	5 618,71	
12-3	International fee Basic fee (first 30 sheets)	b1	2 431,8		
12-4	Remaining sheets		0		
12-5	Additional amount	(X)	53,51		
12-6	Total additional amount	b2	0		
12-7	b1 + b2 =	B	2 431,8		
12-8	Designation fees Number of designations contained in international application		85		
12-9	Number of designation fees payable (maximum 8)		8		
12-10	Amount of designation fee	(X)	523,22		
12-11	Total designation fees	D	4 185,76		
12-12	PCT-EASY fee reduction	R	-749,16		
12-13	Total International fee (B+D-R)	I	⇨	5 868,4	
12-14	Fee for priority document Number of priority documents requested		1		
12-15	Fee per document	(X)	422		
12-16	Total priority document fee	P	⇨	422	
12-17	**TOTAL FEES PAYABLE (T+S+I+P)**		⇨	12 709,11	
12-19	**Mode of payment**		cheque		

VALIDATION LOG AND REMARKS

13-2-6	Validation messages Contents	Green? Reference number for attached copy of general power of attorney not indicated.

PCT (ANNEX - FEE CALCULATION SHEET) 49769

Original (for **SUBMISSION**) - printed on 11.05.2000 09:31:37 AM

13-2-7	**Validation messages** **Fees**	**Green?** **Please verify that modified fee amounts are correct.**

PCT

49769

Original (for **SUBMISSION**) - printed on 11.05.2000 09:31:37 AM

PCT-EASY INFORMATION SHEET

(For applicant use only, DO NOT submit this sheet with the international application)

VALIDATION LOG

	Contents
Green?	Reference number for attached copy of general power of attorney not indicated.
	Fees
Green?	Please verify that modified fee amounts are correct.

Before submitting the International Application, please carefully verify that:

-the information contained on printed Request form is correct;
-Box IX of the Request form has been signed;
-all elements of the international application as indicated in Box VIII of the Request form have been attached; and,
-the diskette containing the PCT-EASY zip file of the International Application has been enclosed and has been clearly labeled "PCT-EASY", with the applicant's or agent's file reference, and the first applicant's name.

ATTENTION

DO NOT modify any indications on the Request form printout. The attached PCT-EASY application has been locked. If an error or an omission is discovered at this time, you must copy the submitted application as a template and make the change or correction in a new application (using the submitted application as a template). You may create such a template by copying the submitted application from the "Stored Forms" folder to the "New PCT Forms" folder. Open the new (.0WO) file created in the "New PCT Forms" folder, correct the errors and proceed with the submission process again.

PATENT COOPERATION TREATY

From the:
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
BERGGREN OY AB
P.O.Box 16
00101 Helsinki
FINLANDE

Berggren Oy Ab
21-02-2001
ML/MM

PCT

WRITTEN OPINION

(PCT Rule 66)

Date of mailing *(day/month/year)*	16.02.2001
Applicant's or agent's file reference: 49769/ML/JK/MM	**REPLY DUE** **within 3 month(s)** from the above date of mailing 16/5/01

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/FI00/00421	11/05/2000	11/05/1999

International Patent Classification (IPC) or both national classification and IPC
H04Q7/38

Applicant
NOKIA NETWORKS OY et al.

1. This written opinion is the **first** drawn up by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

I	☒	Basis of the opinion
II	☐	Priority
III	☐	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
IV	☐	Lack of unity of invention
V	☒	Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
VI	☐	Certain document cited
VII	☒	Certain defects in the international application
VIII	☒	Certain observations on the international application

3. The applicant is hereby **invited to reply** to this opinion.

When? See the time limit indicated above. The applicant may, before the expiration of that time limit, request this Authority to grant an extension, see Rule 66.2(d).

How? By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

Also: For an additional opportunity to submit amendments, see Rule 66.4. For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis. For an informal communication with the examiner, see Rule 66.6.

If no reply is filed, the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: 11/09/2001.

Name and mailing address of the international preliminary examining authority:
European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized officer / Examiner
Harrysson, A

Formalities officer (incl. extension of time limits)
Finnie, A
Telephone No. +49 89 2399 8251

I. Basis of the opinion

1. This opinion has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed".*):

Description, pages:

1-11 as originally filed

Claims, No.:

1-8 as originally filed

Drawings, sheets:

1/2-2/2 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrialapplicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	**1, 4**
Inventive step (IS)	Claims	**1-8**
Industrial applicability (IA)	Claims	

2. Citations and explanations
see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Concerning section V.2 (reasoned statement under Rule 66(a)(ii) PCT)

1 The following documents are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

D1: US 5 475 763 A (CHARLES W. KAUFMAN ET AL) 12 December 1995

D2: US 5 239 294 A (MARY B. FLANDERS ET AL) 24 August 1993

2 With respect to independent **claim 1**, document **D1** discloses (any references in parentheses applying to this document) a method for integrity checking of messages transmitted between a first and a second party, comprising the steps of:

a) calculation of authentication value on basis of the message (see e.g. column 1 at lines 30-32);

b) calculation of authentication value on basis of a counter value, presented as per-message private number (see e.g. column 1 at lines 22-23 and 30-32);

Present claim 1 **differs** from document D1 only in that said claim additionally defines the method steps of:

c) calculation of authentication value on basis of a first value being valid for one connection only and specified by the first party;

d) specifying said counter value at least partly by the second party;

The technical **problem to be solved** by the present invention may be regarded as how to provide security in communication between first and second party in such a way that:

i) a message together with integrity data from one distinct connection is not accepted in the next connection;

ii) values forming the basis for the calculation of authentication values do not have to be stored by both parties.

It is considered that no inventive contribution can be seen in formulating such a problem.

The **solution** proposed in claim 1 of the present application can **not** be considered as **involving an inventive step** (Article 33(3) PCT) for the following reasons:

i) Given the problem (i) stated above, it would be obvious for a skilled person to, without the need of any inventive step, let the long-term private number, which

is already disclosed in **D1** (see e.g. column 1 at lines 30-32), be valid for **only** one connection.

ii) Given the problem (ii) stated above, letting the counter value be stored and thus specified when needed by only one of the parties, for example the second party, is an obvious measure by the skilled person.

The subject-matter of **claim 1** does therefore **not involve an inventive step**.

3 The dependent **claims 2-8** appear to add nothing novel or of inventive significance to those claims to which they are appended.

Particularly letting the parties be a cellular network/mobile station as set out in **claim 2**, is already disclosed for similar authentication procedures in **D2**, see column 1 at lines 18-23. Using pseudo random values as set out in **claim 4** is disclosed in **D1**, column 2 at lines 10-11.

Calculating an authentication value also on the basis of a second value as in **claim 3**, letting a mobile station specify an initial value for the counter value as in **claim 5**, letting a mobile station combine said initial value with a counter value for producing a third value as in **claim 6** or using a value stored in the SIM-card of a mobile station for producing said initial value as in **claim 7**, seems to relate to a routine measures by a skilled person.

Letting the network be an UMTS network and specifying said first value by a radio network controller as in **claim 8**, seems to relate to routine measures by the skilled person not yielding any surprisingly advantageous result.

Thus, the dependent **claims 2-8** either alone or in combination, appear to add **nothing novel or of inventive significance** to claim 1 to which they are appended and, therefore, these claims cannot be considered to offer a basis for a patentable claim. As a consequence, no allowable combination of claims can be suggested by the examiner.

Concerning section VII (defects in form or content)

The following defects are present in the application.

a) If any amended independent claims are filed, the opening part of the description, including the summary of the invention, should be brought into agreement with the wording thereof.

b) In order to meet the requirements of Rule 5.1(a)(ii) PCT, the relevant prior art presumably document **D1** should be acknowledged by reference and briefly discussed in the introductory part of the description.

c) All the claims should include reference signs in parentheses where features shown in the drawings are referred to, Rule 6.2(b) PCT.

d) General "spirit" and "scope" statements are unclear, and when used to interpret the claims renders them also unclear, contrary to Article 6 PCT. The statement of this kind as set out in the last page of the description should therefore be deleted.

e) Finally, amendments should be filed by way of replacement pages in the manner stipulated by Rule 66.8(a) PCT. In particular, fair copies of the amendments should be filed preferably in triplicate. Moreover, the applicant's attention is drawn to the fact that, as a consequence of Rule 66.8(a) PCT the examiner is not permitted to carry out any amendments under the PCT procedure, however minor these may be.

Concerning section VIII (observations on clarity)

The reference to "said third value" in **claim 6** as well as in the description in page 7 at line 6 is considered as being not clear since no third value is mentioned neither in the preceding claims nor in the foregoing text of the description. Also producing a third value as set out in **claim 6** does not seem to have any technical effect since the use of this value is not defined in the claims.

Berggren
ENTTITOIMISTO • PATENT & TRADEMARK ATTORNEYS

Toimitusjohtaja
Managing Director
L. Nordin*

• PATENTIT,
HYÖDYLLISYYSMALLIT:
• PATENTS,
UTILITY MODELS:
J. Kuchanen*
M. Brax*
E. Heikkinen*
T. Laako*
B. Lassenius*
T. Pelin*
I. Risku*
O-P. Saijonmaa*
J. Svensson*
P. Tennua*
B. Träskman*
M. Karttunen
S. Kuisma
M. Laajalahti
K. Suominen
V. Tognetty
S. Vatalo

• MALLIT:
• DESIGNS:
L. Vaitakka

• TAVARAMERKIT,
LAKIASIAT:
• TRADEMARKS,
LEGAL MATTERS:
P. Kolve**
S. Henn**
I. Karlsson**
H. Halmetoja**
E-M. Söderström**
S. Ascola
J. Tanttie

29 March 2001

European Patent Office
D-80298 Munich
Germany

Our Ref.: 49769/MB/MM

REPLY TO WRITTEN OPINION
INTERNATIONAL PATENT APPLICATION NO. PCT/FI00/00421
APPLICANT: NOKIA NETWORKS OY
TERM: 16 MAY 2001

In response to the Written Opinion dated 16 February 2001 we submit the following.

The applicant respectfully disagrees with the Examiner about the alleged pertinence of D1.

Firstly, the applicant wants to contest the Examiner's opinion about it being obvious that the long-term private (or secret) number introduced in D1 could be valid for one connection only. The disclosure of D1 rests solidly on the basis of PKI (Public Key Infrastructure), where the keys constitute pairs of public and secret keys. The needlessly complicated designations "long-term private number" or "long-term secret number" of D1 simply refer to the message originator's secret key. The keys of PKI are definitely long-term by nature as already the name used in D1 suggests. The applicant would like to point out that D1 specifically discloses the use of per-message secret numbers because a person skilled in the art would not contemplate sacrificing a long-term key for one-time use. A factor that is conveniently ignored in D1 but that is both common knowledge and a good argument in favour of the applicant's opinion is that a recipient that receives the corresponding public key or "long-term public number" must somehow ascertain that what he has received really comes from the party that claims to be the originator and not from a dishonest pretender. It would be very difficult if not impossible to arrange for proper authentication of keys if the "long-term numbers" of D1 would not be long-term at all but only message specific.

erggren Oy Ab
oite • Address:
16 • P.O.Box 16
-00101 Helsinki
LAND
Käyntiosoite • Office:
Graniittitalo
Jaakonkatu 3 A
Helsinki
Nat. 09) 693 701
Int. +358 9 693 701
Fax +358 9 693 3944
email.box@berggren.fi
http://www.berggren.fi
Pankit • Bankers:
MERITA 157330-15411
SWIFT MRITFIHH
LEONIA 800017-90104
SWIFT PSPBFIHH
Yhtiö • Company:
Kotipaikka Helsinki
Trade Reg. No. 30.302
ALV 0107002-7
VAT FI01070027

Secondly, and even more importantly, the applicant would like to point out that the method taught in D1 is hopelessly powerless against a so-called replay attack, which means that a dishonest party somehow manages to record a message during transmission and resends it later to the same recipient as if it was a valid message from the real originator. Quite on the contrary, D1 acknowledges literally on lines 55-60 of column 2 that resending the same message later would result in the signature being the same, which means that the poor recipient has no means of finding out, whether the latter message was a proper resent copy from the real originator or whether it was a replayed echo from an unknown heckler. D1 goes as far as describing such a feature as "desirable"!

Said severe drawback of the D1 method is at least partly a consequence of the fact that D1 only discloses transmission of various pieces of information *from* the originator *to* the recipient. If we now move on to use the designations that appear in the pending claims, we note firstly that the independent claim only mentions *one* authentication value on line 2, after which the later reference to the same concept on line 6 comes with the definite article "the". It is the one and only authentication value the ingredients of which are a) the message itself, b) a first, message specific value specified by the first party AND c) a counter value at least partly specified by the second party, i.e. the recipient. Ingredient c) has no antecedent basis in the cited reference publications. Taken that we only speak about one authentication value, the calculation of which takes place in one location (at the first party, or "originator"), it is evident that the counter value must be provided from the second party (recipient) to the first party (originator) prior to the calculation of the authentication value. No cited reference publication discloses the transmission of a counter value from the recipient to the originator prior to calculating an authentication value.

In the light of the above-given argumentation the applicant would respectfully request positive reconsideration of the merits of the application in unamended form..

BERGGREN OY AB

Matti Brax
Patent Attorney

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

mm | ML

Berggren Oy Ab

PCT 08 -05- 2001

To:

BERGGREN OY AB
P.O.Box 16
00101 Helsinki
FINLANDE

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

Applicant's or agent's file reference 49769/ML/JK/MM	Date of mailing *(day/month/year)* 04.05.2001
	IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/FI00/00421	11/05/2000	11/05/1999

Applicant
NOKIA NETWORKS OY et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Finnie, A Tel.+49 89 2399-8251

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
49769/ML/JK/MM		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/FI00/00421	11/05/2000	11/05/1999
International Patent Classification (IPC) or national classification and IPC H04Q7/38		
Applicant NOKIA NETWORKS OY et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
07/12/2000	04.05.2001
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Harrysson, A Telephone No. +49 89 2399 7529

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/FI00/00421

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:
Description, pages:

1-11	as originally filed

Claims, No.:

1-8	as originally filed

Drawings, sheets:

1/2-2/2	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   - ☐ the description, pages:
   - ☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims 1-8
	No:	Claims
Inventive step (IS)	Yes:	Claims 1-8
	No:	Claims
Industrial applicability (IA)	Yes:	Claims 1-8
	No:	Claims

2. Citations and explanations
see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Concerning section V (reasoned statement under Article 35(2) PCT)

1 **Claim 1** defines a method for integrity checking of messages transmitted between a first and a second party. The nearest prior art is represented by document **D1 (US 5 475 763)** which discloses such a method wherein an authentication value is calculated on basis of the message (see D1 column 1 at lines 30-32) and on basis of a counter value, presented as per-message private number (see D1 column 1 at lines 22-23 and 30-32);

Present claim 1 **differs** from document D1 in that said claim additionally defines the method steps of calculation an authentication value on basis of a first value being valid for one connection only and specified by the first party, and specifying said counter value at least partly by the second party.

The technical **problem to be solved** by the present invention may be regarded as how to provide security in communication between first and second party in such a way that a message together with integrity data from one distinct connection is not accepted in the next connection and values forming the basis for the calculation of authentication values do not have to be stored by both parties.

The **solution** proposed in claim 1 of the present application is considered as **involving an inventive step** since letting the second party specify a value, this value being a counter value, is neither taught nor suggested by D1. A so called replay attack can therefore be encountered by the subject-matter of the application, but not by the method of D1.

The claimed method is also neither taught nor suggested by the remaining documents cited in the search report.

Thus the subject-matter of **claim 1** is considered novel, industrially applicable and inventive in the sense of Article 33 PCT.

2 The dependent **claims 2-8** all relate to further implementing details of claim 1 and are therefore also novel, inventive and industrially applicable.

Concerning section VII (defects in form or content)

The following defects are present in the application.

In order to meet the requirements of Rule 5.1(a)(ii) PCT, the relevant prior art, document **D1**, should have been acknowledged by reference and briefly discussed in the introductory part of the description.

The claims do not include reference signs in parentheses where features shown in the drawings are referred to, contrary to Rule 6.2(b) PCT.

General "spirit" and "scope" statements are unclear, and when used to interpret the claims renders them also unclear, contrary to Article 6 PCT. The statement of this kind as set out in the last page of the description should have been deleted.

Concerning section VIII (observations on clarity)

The reference to "said third value" in **claim 6** as well as in the description in page 7 at line 6 is considered as being not clear since no third value is mentioned neither in the preceding claims nor in the foregoing text of the description. Also producing a third value as set out in **claim 6** does not seem to have any technical effect since the use of this value is not defined in the claims.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 49769	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/FI 00/00421	International filing date *(day/month/year)* 29 May 2000	(Earliest) Priority Date *(day/month/year)* 11 May 1999
Applicant NOKIA NETWORKS OY		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. [ ] **Certain claims were found unsearchable** (See Box I).

2. [ ] **Unity of invention is lacking** (See Box II).

3. [ ] The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing
   - [ ] filed with the international application.
   - [ ] furnished by the applicant separately from the international application,
     - [ ] but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
   - [ ] transcribed by this Authority.

4. With regard to the title,
   - [X] the text is approved as submitted by the applicant.
   - [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   - [X] the text is approved as submitted by the applicant.
   - [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:

   Figure No. 1
   - [X] as suggested by the applicant.
   - [ ] because the applicant failed to suggest a figure.
   - [ ] because this figure better characterizes the invention.
   - [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00421

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0798673 A1 (KONINKLIJKE PTT NEDERLAND N.V.), 1 October 1997 (01.10.97), column 1, line 46 - column 2, line 49; column 4, line 1 - column 7, line 29, figure 6, claims 1,2,8, abstract	1,3
A	--	2,4-8
Y	US 5475763 A (CHARLES W. KAUFMAN ET AL), 12 December 1995 (12.12.95), column 2, line 35 - column 3, line 4, figure 1, claims 1-12, abstract	1,3
A	--	2,4-8

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2000	29. 09. 2000

Name and mailing address of the International Searching Authority
European Patent Office P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel(+31-70)340-2040, Tx 31 651 epo nl,
Fax(+31-70)340-3016

Authorized officer
Klas Arvidsson/mj
Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00421

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9421066 A1 (TELSTRA CORPORATION LIMITED), 15 Sept 1994 (15.09.94), page 3, line 22 - page 4, line 15, figure 1, claim 1, abstract	1,3
A	--	2,4-8
A	US 5369707 A (ROY D. FOLLENDORE, III), 29 November 1994 (29.11.94), column 2, line 60 - column 4, line 8, figure 4, claims 1-28, abstract	1,3,4
	--	
A	US 5239294 A (MARY B. FLANDERS ET AL), 24 August 1993 (24.08.93), column 4, line 29 - column 5, line 68, figures 2,3, claims 1-32, abstract	1,3,4
	--	
A	US 5592553 A (RICHARD H. GUSKI ET AL), 7 January 1997 (07.01.97), column 2, line 63 - column 4, line 9, figure 3, claims 1-31, abstract	1,3,4
	--	
A	US 5757919 A (HOWARD C. HERBERT ET AL), 26 May 1998 (26.05.98), column 1, line 58 - column 2, line 5; column 6, line 31 - column 7, line 22, figures 5a,b, claims 1-24, abstract	1,3,4
	--	

INTERNATIONAL SEARCH REPORT

Information on patent family members

08/05/00

International application No.
PCT/FI 00/00421

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0798673 A1	01/10/97	AU 712353 B	04/11/99
		AU 2506297 A	22/10/97
		CA 2245921 A	09/10/97
		CN 1215489 A	28/04/99
		CZ 9802956 A	17/02/99
		EP 0960404 A	01/12/99
		JP 11506560 T	08/06/99
		NO 984535 A	28/09/98
		NZ 331258 A	28/10/99
		WO 9737331 A	09/10/97
US 5475763 A	12/12/95	NONE	
WO 9421066 A1	15/09/94	AU 683646 B	20/11/97
		AU 6255694 A	26/09/94
US 5369707 A	29/11/94	CA 2101198 A	28/07/94
US 5239294 A	24/08/93	AU 6034790 A	06/02/91
		CA 2063447 A,C	13/01/91
		IL 94467 A	31/12/95
		JP 2684118 B	03/12/97
		JP 5503816 T	17/06/93
		MX 166091 B	17/12/92
		WO 9101067 A	24/01/91
		CA 2087433 A,C	17/01/92
		JP 2750638 B	13/05/98
		MX 9100231 A	28/02/92
		WO 9202103 A	06/02/92
		US 5572193 A	05/11/96
US 5592553 A	07/01/97	EP 0636963 A	01/02/95
		JP 7107086 A	21/04/95
		US 5661807 A	26/08/97
US 5757919 A	26/05/98	AU 5688998 A	03/07/98
		DE 19782169 T	28/10/99
		GB 2334866 A	01/09/99
		GB 9912947 D	00/00/00
		WO 9826535 A	18/06/98

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04Q 7/38, H04L 9/32 — A1

(11) International Publication Number: **WO 00/69206**

(43) International Publication Date: 16 November 2000 (16.11.00)

(21) International Application Number: PCT/FI00/00421

(22) International Filing Date: 11 May 2000 (11.05.00)

(30) Priority Data:
991088 11 May 1999 (11.05.99) FI

(71) Applicant *(for all designated States except US)*: NOKIA NETWORKS OY [FI/FI]; P.O. Box 300, FIN–00045 Nokia Group (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: NIEMI, Valtteri [FI/FI]; Itämerenkatu 11–13, FIN–00180 Helsinki (FI). RAJANIEMI, Jaakko [FI/FI]; Lapinrinne 2 A 11, FIN–00180 Helsinki (FI). MUHONEN, Ahti [FI/FI]; Holperintie 39, FIN–04680 Hirvivaara (FI).

(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN–00101 Helsinki (FI).

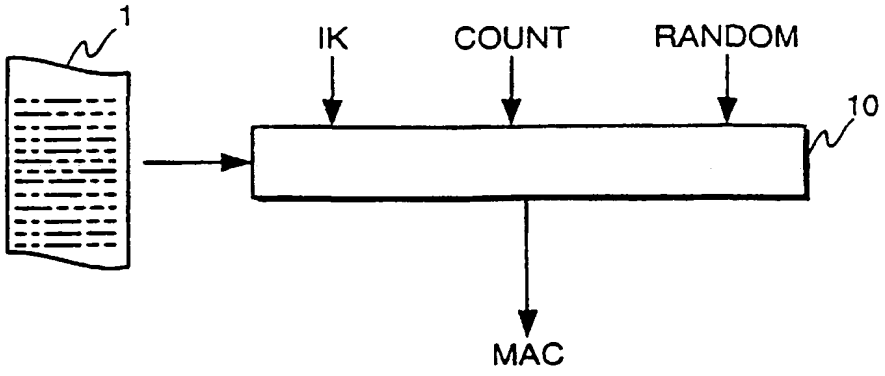
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: INTEGRITY PROTECTION METHOD FOR RADIO NETWORK SIGNALING

(57) Abstract

The invention is directed to a method for checking the integrity of messages between a mobile station and the cellular network. Two time–varying parameters are used in MAC calculation, one of which is generated by the mobile station, and the other by the network. The parameter specified by the network is used in one session only, and is transmitted to the mobile station in the beginning of the connection. The parameter specified by the mobile station is stored in the mobile station between connections in order to allow the mobile station to use a different parameter in the next connection. The parameter specified by the mobile station is transmitted to the network in the beginning of the connection.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Integrity protection method for radio network signaling

TECHNICAL FIELD OF THE INVENTION

The invention is directed to a method for checking the integrity of messages between a mobile station and the cellular network. Particularly, the invention is directed to such a method as described in the preamble of Claim 1.

BACKGROUND OF THE INVENTION

All telecommunication is subject to the problem of how to make sure that the received information is sent by an authorized sender and not by somebody who is trying to masquerade as the sender. The problem is evident in cellular telecommunication systems, where the air interface presents an excellent platform for eavesdropping and replacing the contents of a transmission by using higher transmission levels, even from a distance. A basic solution to this problem is authentication of the communicating parties. An authentication process aims to discover and check the identity of both of the communicating parties, so that each party receives information about the identity of the other party, and can trust the identity to a sufficient degree. Authentication is typically performed in a specific procedure at the beginning of the connection. However, this leaves room for unauthorized manipulation, insertion, and deletion of subsequent messages. Thus, there is a need for separate authentication of each transmitted message. The latter task can be done by appending a message authentication code (MAC) to the message at the transmitting end, and checking the MAC value at the receiving end.

A MAC is typically a relatively short string of bits, which depends in some specified way on the message it protects and on a secret key known both by the sender and by the recipient of the message. The secret key is generated and agreed typically in connection with the authentication procedure in the beginning of the connection. In some cases the algorithm that is used to calculate the MAC based on the secret key and the message is also secret but this is not usually the case.

The process of authentication of single messages is often called integrity protection. To protect the integrity of signaling, the transmitting party computes a MAC value based on the message to be sent and the secret key using the specified algoritm, and sends the message with the MAC value. The receiving party recomputes a MAC value based on the message and the secret key according to the specified algorithm,

and compares the received MAC and the calculated MAC. If the two MAC values match, the recipient can trust that the message is intact and sent by the supposed party. One may note in passing, that integrity protection does not usually include protection of confidentiality of the transmitted messages.

Integrity protection schemes are not completely perfect. A third party can try to manipulate and succeed in manipulating a message transmitted between a first and a second party. There are two main alternative methods for forging a MAC value for a modified or a new messages, namely by obtaining the secret key first, and by trying directly without the secret key.

The secret key can be obtained by a third party basically in two ways:
- by computing all possible keys until a key is found, which matches with data of observed message-MAC pairs, or by otherwise breaking the algorithm for producing MAC values; or
- by directly capturing a stored or transmitted secret key.

The original communicating parties can prevent a third party from obtaining the secret key by using an algorithm that is cryptographically strong and which uses a long enough secret key to prevent exhaustive search of all keys, and using other security means for transmission and storage of secret keys.

A third party can try to disrupt messaging between the two parties without a secret key basically by guessing the correct MAC value, or by replaying of some earlier message transmitted between the two parties, for which message the correct MAC is known from the original transmission.

Correct guessing of the MAC value can be prevented by using long MAC values. The MAC value should be long enough to reduce the probability of guessing right to a sufficiently low level compared to the benefit gained by one successful forgery. For example, using a 32 bit MAC value reduces the probability of a correct guess to 1 / 4 294 967 296, which is small enough for most applications.

Obtaining a correct MAC value using the replay attack i.e. by replaying an earlier message can be prevented by introducing a varying parameter to the calculation of the MAC values. For example, a time stamp value, a sequence number, or a random number can be used as a further input to the MAC algorithm in addition to the secret integrity key and the message. The present invention is associated with this basic method. In the following, the prior art methods are described in more detail.

When using a time stamp value, each communicating party needs to have an access to a reliable clock in order to be able to calculate the MAC in the same way. The problem with this approach is the need of the reliable clock. The clocks of both parties must be very accurate and be very accurately in time. However, this condition is unacceptable in cellular telecommunication systems: both parties, i.e. the mobile station (MS) and the network do not have access to a clock, that is reliable enough.

When using sequence numbers, each party has to keep track of those sequence numbers that have already been used and are not acceptable any more. The easiest way to implement this is to store the highest sequence number used in MAC calculations so far. This approach has the drawback, that between connections each party must maintain state information which is at least to some level synchronized. That is, they need to store the highest sequence number used so far. This requires the use of a large database at the network side.

A further approach is to include a random number in each message, which the other side must use in MAC calculation when for the next time sending a message, for which MAC authentication is required. This approach has the same drawback as the previous one, i.e. between connections each party must maintain state information, which requires the use of a large database at the network side.

SUMMARY OF THE INVENTION

An object of the invention is to realize a method for integrity checking, which avoids the problems associated with prior art. A further object of the invention is to provide a method for integrity checking, which does not require storage of state information on the network side.

The objects are reached by using two time-varying parameters in MAC calculation, one of which is generated by the mobile station, and the other by the network. The parameter specified by the network is used in one session only, and is transmitted to the mobile station in the beginning of the connection. The parameter specified by the mobile station is stored in the mobile station between connections in order to allow the mobile station to use a different parameter in the next connection. The parameter specified by the mobile station is transmitted to the network in the beginning of the connection.

The method according to the invention is characterized by that, which is specified in the characterizing part of the independent method claim. The dependent claims describe further advantageous embodiments of the invention.

According to the invention, both parties specify a varying parameter to be used in the generation of MAC values. On the network side in a mobile network, all state information about the particular user can be discarded after the connection is released. According to the invention, both a sequence number and a network specified value such as a pseudorandom number is used in calculation of the MAC value. In the beginning of the connection, the mobile station determines the initial value used for the sequence counting, and transmits the value to the network. In addition to the initial value, a counter value is used. The initial value and the counter value are concatenated, added or combined in some other way to produce the parameter to be used in the calculation of the MAC value of a message. One way of combining the two values is using the initial value as the starting value of the counter, which corresponds to the addition of the counter value and the initial value. The invention does not limit which counter values are used in the inventive method. A suitable value is for example the protocol data unit (PDU) number of the radio link control (RLC) protocol, i.e. the RLC PDU number. Another suitable value is the use of a counter, which is incremented at fixed intervals, for example every 10 milliseconds. Preferably, a counter such as the RLC PDU counter which is already present in mobile stations and in the network is used in a method according to the invention. Further, also counters associated with ciphering of data over the radio interface can be used in a method according to the invention. Further, the invention does not limit which initial value is used in the inventive method. For example, the current hyperframe number at the time of initiating of the connection can be used as the initial value. Further, the counter values do not need to be transmitted after the transmission of the initial value, since both sides of the connection can update the counters in the same way during the connection, preserving synchronization. Preferably, when a connection is released, the mobile station stores into its memory the initial value used in the connection or at least the most significant bits of the initial value, which allows the mobile station to use a different initial value next time. The mobile station can save the information for example in the SIM (Subscriber Identity Module) card or another memory device, for allowing the mobile station to use a value previously stored in the SIM card of the mobile station in specifying the initial value.

The network specifies the random number, or in practice a pseudorandom number in the beginning of the connection. The random number is session specific, i.e. it does not need to be changed within a connection or transmitted to the mobile station more than once in the beginning of the connection, and neither does it need to be stored in the network between connections. Advantageously, the network element generating the random number and taking care of MAC value generation and checking of received messages and MAC values is the radio network controller (RNC). However, the invention is not limited to that, since these functions can be realized in many other network elements as well. The use of RNC is advantageous, since in that case the core network of the cellular telecommunication system does not need to participate in integrity checking of single messages, and since radio access network messaging may also need to be protected by integrity checking.

The invention allows both sides of the connection to perform integrity checking. Since the network specifies a random value in the beginning of the connection, a mobile station of a hostile party cannot succesfully perform a replay attack by replaying a message recorded from a previous connection. Since the mobile station specifies the initial value for the connection, replay attacks from a bogus network element operated by a hostile party will not succeed.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described in more detail in the following with reference to the accompanying drawings, of which

Figure 1 illustrates an advantageous embodiment of the invention,

Figure 2 illustrates a method according to an advantageous embodiment of the invention, and

Figure 3 illustrates signalling according to an advantageous embodiment of the invention.

Same reference numerals are used for similar entities in the figures.

DETAILED DESCRIPTION

Figure 1 illustrates a way of calculating the MAC value according to the invention. The IK is the secret integrity key, which is generated during a mobile station authentication procedure in the beginning of a connection. Because the same IK key is used to authenticate many messages possibly even during many consecutive

connections, time-varying parameters are needed to avoid hostile attacks during the connection. For that purpose, a counter value COUNT and a random value RANDOM are used in the MAC calculation as well. According to the invention, a message 1 and the IK, COUNT, and RANDOM values are input into a calculation means 10, which calculates a MAC value according to the inputs and the particular authentication algorithm. We note here, that the invention is not limited to any specific way of calculating the MAC value from the inputs illustrated in figure 1. The invention is not limited to any specific lengths of the input values. For example, for the UMTS (Universal Mobile Telecommunication System) cellular system suitable lengths are 128 bits for the IK value, 32 bits for the COUNT value, 32 bits for the RANDOM value, and 16 bits for the MAC value. However, other lengths could be used even for the UMTS system, and other inputs can be used in addition to these values.

If a new IK value is generated in an authentication process in the beginning of the current connection, the mobile station can reset the initial value of COUNT, since new IK value provides security against replay attacks. The storing of the initial value or a part of it for use with the next connection is necessary, since the IK value might not change, when the next connection is established. This is very probable for example when using a multifunction mobile station in the UMTS system, since the mobile station can have multiple simultaneous connections of various types, and establish and release new connections during a single communication session. The network does not necessarily perform full authentication for each new connection, whereby the mobile station will not always receive a new IK value for each new connection. However, when the IK is changed, the mobile station can reset the initial COUNT values without danger of compromising security.

Figure 2 illustrates a method according to an advantageous embodiment of the invention. Figure 2 illustrates a method for integrity checking of a message transmitted during a connection between a cellular telecommunication network and a mobile station.

In the first step 50, the transmitting party calculates the authentication value (MAC) of the message on the basis of the message, a first value specified by the network, said first value being valid for one connection only, a second value specified at least in part by the network, and a third value at least partly specified by the mobile station. Preferably, said first value is a pseudorandom value such as the RANDOM value described previously. Further, said third value is preferably a counter value such as the COUNT value described previously, which value is incremented during

the connection. For example, the RLC PDU value can be used for generation of the COUNT value. As described previously, the mobile station specifies an initial value for the counter value in the beginning of the connection. The initial value can be used as a starting value for a counter producing the COUNT values, or the initial value can be combined with some other counter value such as the RLC PDU value for producing said third value.

In the next step 52, the message is transmitted from the transmitting party to the receiving party, which calculates a second MAC value as described previously, and compares the received MAC value and the calculated MAC value in step 56. If they are found to be equal, the message is accepted in step 58, and if they are found to be unequal, the message is rejected in step 60. In the case of uplink messaging, the steps of calculation 54 and comparison 56 can advantageously be performed by a radio network controller in the cellular telecommunication network. The method of figure 2 is used for checking the integrity of at least some of uplink and downlink messages.

Figure 3 illustrates one example of how to initiate a connection according to an advantageous embodiment of the invention. Figure 3 shows an advantageous solution to the problem of how to exchange two initial values for the purposes of integrity checking. We note here that the signalling sequence shown in figure 3 is in no way limited to passing only the COUNT and RANDOM values described previously. Signalling according to figure 3 can be used for exchange of any two keys in the beginning of a connection. Figure 3 shows as an example signalling associated with a mobile originated call, but corresponding signalling sequences can be used also in other situations, such as in establishing a mobile terminating call, or in a paging response procedure.

Figure 3 shows a particular example of a method according to the invention. The central idea in figure 3 is, that the RNC stores the message or messages received from the mobile station and authenticated with a MAC value until the time, when it is able to check the MAC value of the message(s). If one or all of the MAC values are later found to be false, the network can then decide, if it should discard the initiated connection.

Figure 3 illustrates signalling between a mobile station MS 20, a radio network controller RNC 30, and core network CN 40 in a situation, in which the mobile station initiates a connection. Figure 3 illustrates the signalling using terminology of the UMTS system. In the first step 100, the mobile station sends the initial

connection request message RRC SETUP REQ to the network. After receiving the connection request message, the RNC generates the RANDOM value, after which the RNC replies by sending 105 an acknowledgment message ACK to the mobile station. The RNC specifies the RANDOM value to the mobile station by attaching the value as a parameter to the ACK message, which is shown in figure 3 by the label RANDOM appearing under the arrow 105. After receiving the acknowledgment and the RANDOM value, the mobile station needs to send the initial COUNT value to the network. This can be realized basically in two ways: by defining a new message for that purpose, for example in the RRC level, or by attaching the COUNT value as a parameter to an existing message. Arrow 110 denotes the former approach, i.e. denotes a message specifically defined for transmitting the COUNT value. Arrow 115 denotes the latter approach, i.e. attaching the COUNT value as a parameter to an existing message. In the example of figure 3, the existing message is a CM SERV REQ message. Further, also an IK key identification number may be transmitted as a parameter to the message. During an authentication process in which an IK is generated, each IK is assigned an identification number, whereafter the MS and the network may refer to the IK simply by using the identification number.

In the example of figure 3, the mobile station sends a classmark service request message CM SERV REQ to the network, specifying a temporary identifier TMSI and a capability class identifier CM2 to the network. If a specific message was not used to transport the initial COUNT value to the network, the initial COUNT value is passed to the network as a further parameter to the CM SERV REQ message. Further, the mobile station transmits a MAC value calculated on the basis of the COUNT and RANDOM values, and an IK value received and stored during a previous connection. Upon receiving the message, the RNC removes and stores the MAC value from the message as well as the possibly existing COUNT value, and forwards 120 the rest of the message to the core network. The RNC stores the whole message as well for later use, which will be described later. According to UMTS specifications, the core network may perform an authentication procedure at this stage, which is represented by arrows 125 and 130 in figure 3, corresponding to authentication request AUTH REQ and authentication response AUTH RSP messages.

The next step depends on whether the network has an IK value for the mobile station or not. If the network performed the authentication in steps 125 and 130, the network has the IK value determined in the authentication. Alternatively, the

network may have an old IK value stored in relation to a previous connection. The IK value is stored in the core network registers. If the network has an IK value, the method continues at step 135; if not, at step 150. This is represented by step 132 and the associated dashed arrow in figure 3.

In step 135, the core network sends a ciphering mode CIPH MODE message to the RNC, attaching the ciphering key CK and the IK value as parameters to the message. With this message, the CN supplies the IK value to the RNC, which was previously unaware of the IK value, if the authentication procedure was not performed at steps 125 and 130. At this stage, the RNC is able to check the CM SERV REQ message stored at step 115, since it now has the COUNT, the RANDOM, and the IK values necessary for calculating the MAC value of the message. The RNC calculates a MAC value and compares 137 it to the MAC value stored previously at step 115. If the match, the method continues at step 140. If they do not match, the method continues at step 160.

In step 140, the RNC sends to the MS a CIPHERING COMMAND message to start ciphering, to which the MS replies 145 by sending a ciphering response message CIPHERING RSP back to RNC. After that, the communication continues normally, and the continuation is not depicted in figure 3.

In step 150, the network performs an authentication process, which is represented by arrows 150 and 155 in figure 3, corresponding to authentication request AUTH REQ and authentication response AUTH RSP messages. After that, the core network informs the RNC about the new IK (not shown).

At this stage the RNC needs to make sure, that the MS is the correct one and can calculate the MAC values accordingly. The RNC can perform for example a classmark request procedure or some other suitable procedure to that effect. That is, the RNC sends 160 a classmark request CLASSMARK REQ message to the MS, which replies by sending 165 a response message RSP back to the RNC, attaching the classmark information CM2 as a parameter to the message, and the calculated MAC value at the end of the message. Now the RNC can again check the MAC, and if no hostile party has replayed any of the previous messages, the MAC values calculated by the RNC and the MS will match, since the three key values IK, RANDOM, and COUNT are now known both to the MS and the RNC. After receiving the classmark response message RSP, the RNC sends 170 the classmark information in a CLASSMARK message to the core network, as required by the UMTS specifications.

Although in the previous description, the network is described to specify a random number to be used as the network-specified varying parameter, also other than random values can be used. For example, although being a less advantageous example of an embodiment of the invention, the network may use a counter value, and store the counter value in a central register in order to be able to use a different value during the next connection. Naturally, this embodiment has the disadvantage of the burden of storage of the values of the users to be used in the following connections.

In the previous examples, the invention has been described in relation to a cellular telecommunication system. The invention can be very advantageously used in such a system, since it requires very little messaging, and thus uses only a diminutive amount of valuable air interface resources. However, the invention can be applied also in other communication systems.

The invention has several advantages. For example, according to most advantageous embodiments there is no need for maintaining synchronized state information between different connections. That is, these embodiments do not require the network to store any counter information for effecting the integrity checking which is a considerable advantage, since such storage would have to be effected in a central register such as the VLR (Visitor Location Register) or the HLR (Home Location Register). According to these most advantageous embodimetnts, all state information about the connection can be discarded on the network side in a mobile network after the connection is released. The invention allows the integrity checking to be performed by a network element outside the core network, such as the RNC in the case the UMTS cellular system.

The invention does not specify any upper limit for the number of values used in calculation of MAC values. Any other values in addition to those described for example in relation to figure 1 may be used as well. Further, the invention does not limit, which messages are subjected to integrity checking: all messages, a certain group of messages, or messages selected in some other way.

The name of a given functional entity, such as the radio network controller, is often different in the context of different cellular telecommunication systems. For example, in the GSM system the functional entity corresponding to a radio network controller (RNC) is the base station controller (BSC). Therefore, the term radio network controller is intended to cover all corresponding functional entities regardless of the term used for the entity in the particular cellular tele-

communication system. Further, the various message names such as the RRC SETUP REQ message name are intended to be examples only, and the invention is not limited to using the message names recited in this specification.

In view of the foregoing description it will be evident to a person skilled in the art that various modifications may be made within the scope of the invention. While a preferred embodiment of the invention has been described in detail, it should be apparent that many modifications and variations thereto are possible, all of which fall within the true spirit and scope of the invention.

Claims

1. Method for integrity checking of messages transmitted during a connection between a first party and a second party, in which method an authentication value is calculated for a message,
characterized in that the method comprises steps, in which
the authentication value of a message is calculated on the basis of
- the message,
- a first value specified by the first party, said first value being valid for one connection only,
- a counter value at least partly specified by the second party.

2. A method according to claim 1, **characterized** in that said first party is a cellular telecommunication network and said second party is a mobile station.

3. A method according to claim 1, **characterized** in that the authentication value of a message is calculated also on the basis of a second value specified at least in part by the first party.

4. A method according to claim 1, **characterized** in that said first value is a pseudorandom value.

5. A method according to claim 2, **characterized** in that the mobile station specifies an initial value for the counter value.

6. A method according to claim 2, **characterized** in that the mobile station specifies an initial value which is combined with a counter value for producing said third value.

7. A method according to claim 5, **characterized** in that the mobile station uses a value previously stored in the SIM card of the mobile station in specifying said initial value.

8. A method according to claim 1, **characterized** in that said cellular telecommunication network is an UMTS network, and said first value is specified by a radio network controller.

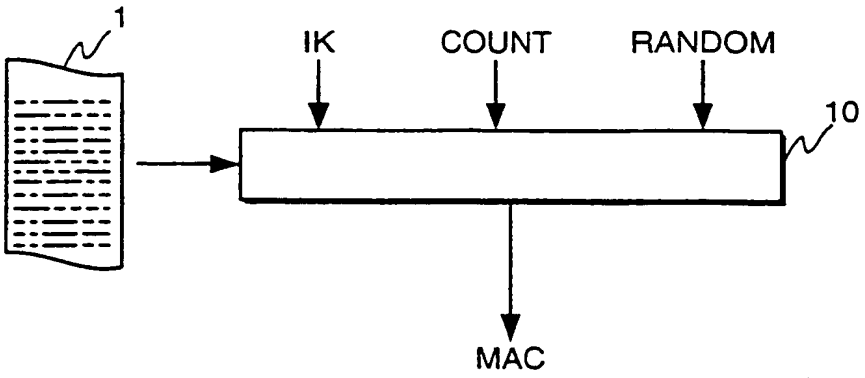

1
IK
COUNT
RANDOM
10
MAC

Fig. 1

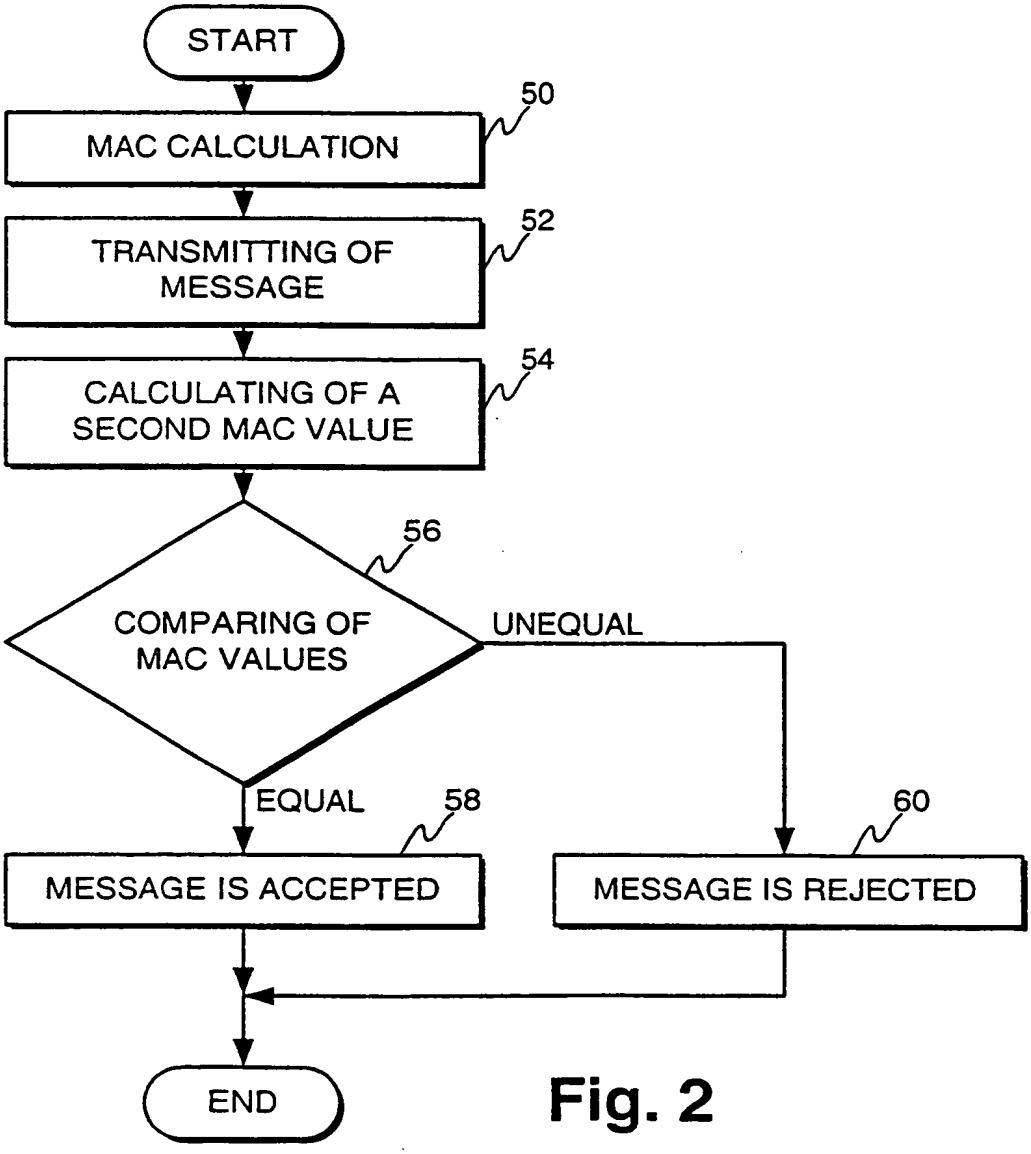

START
MAC CALCULATION
50
TRANSMITTING OF MESSAGE
52
CALCULATING OF A SECOND MAC VALUE
54
COMPARING OF MAC VALUES
56
UNEQUAL
EQUAL
58
60
MESSAGE IS ACCEPTED
MESSAGE IS REJECTED
END

Fig. 2

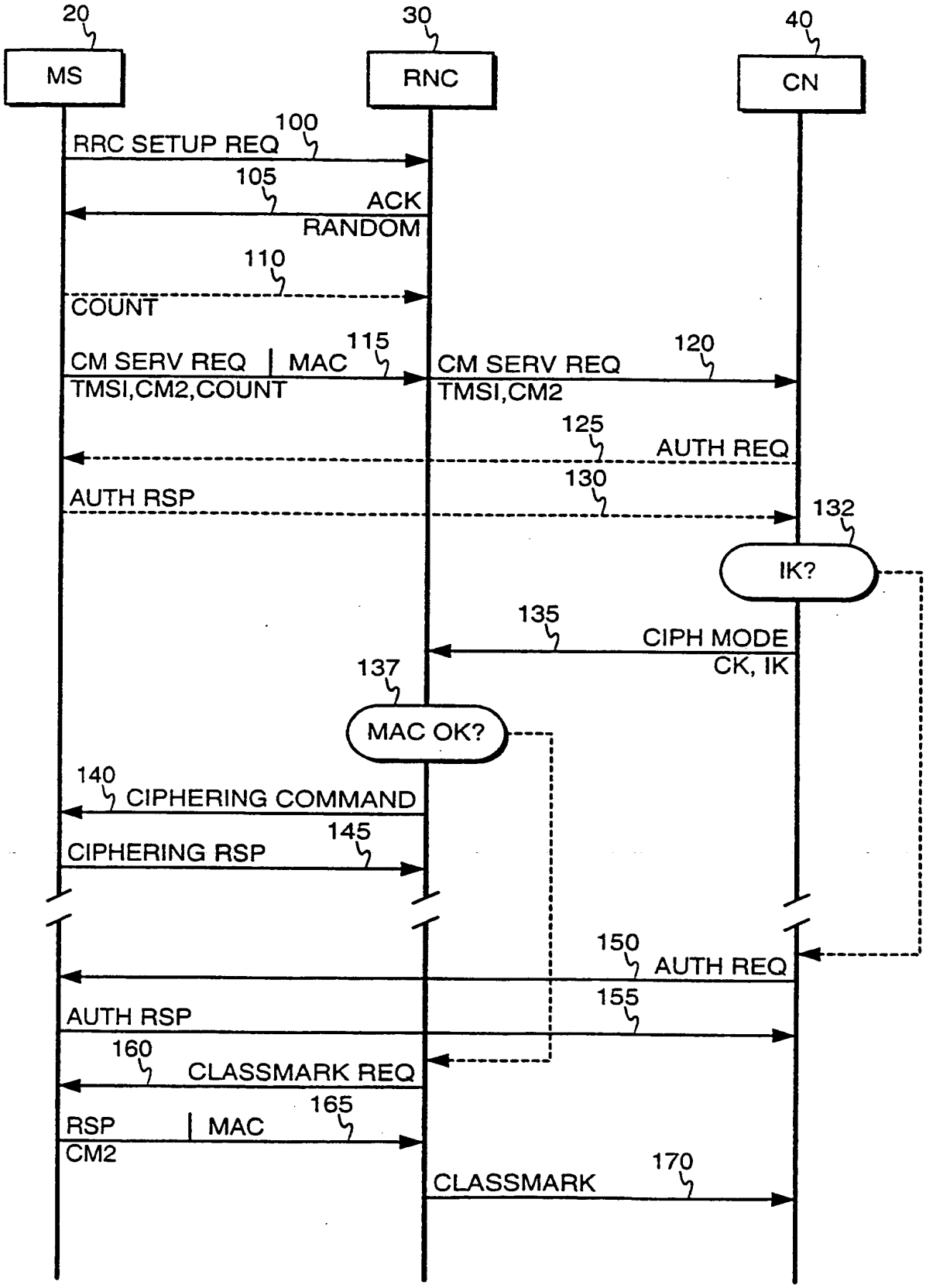

20
MS
30
RNC
40
CN
100
RRC SETUP REQ
105
ACK
RANDOM
110
COUNT
115
CM SERV REQ | MAC
TMSI,CM2,COUNT
120
CM SERV REQ
TMSI,CM2
125
AUTH REQ
130
AUTH RSP
132
IK?
135
CIPH MODE
CK, IK
137
MAC OK?
140
CIPHERING COMMAND
145
CIPHERING RSP
150
AUTH REQ
155
AUTH RSP
160
CLASSMARK REQ
165
RSP | MAC
CM2
170
CLASSMARK

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00421

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0798673 A1 (KONINKLIJKE PTT NEDERLAND N.V.), 1 October 1997 (01.10.97), column 1, line 46 - column 2, line 49; column 4, line 1 - column 7, line 29, figure 6, claims 1,2,8, abstract	1,3
A	--	2,4-8
Y	US 5475763 A (CHARLES W. KAUFMAN ET AL), 12 December 1995 (12.12.95), column 2, line 35 - column 3, line 4, figure 1, claims 1-12, abstract	1,3
A	--	2,4-8

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2000	29 09 2000

Name and mailing address of the International Searching Authority
European Patent Office P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel(+31-70)340-2040. Tx 31 651 epo nl.
Fax(+31-70)340-3016

Authorized officer
Klas Arvidsson/mj
Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00421

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9421066 A1 (TELSTRA CORPORATION LIMITED), 15 Sept 1994 (15.09.94), page 3, line 22 - page 4, line 15, figure 1, claim 1, abstract	1,3
A	--	2,4-8
A	US 5369707 A (ROY D. FOLLENDORE, III), 29 November 1994 (29.11.94), column 2, line 60 - column 4, line 8, figure 4, claims 1-28, abstract	1,3,4
	--	
A	US 5239294 A (MARY B. FLANDERS ET AL), 24 August 1993 (24.08.93), column 4, line 29 - column 5, line 68, figures 2,3, claims 1-32, abstract	1,3,4
	--	
A	US 5592553 A (RICHARD H. GUSKI ET AL), 7 January 1997 (07.01.97), column 2, line 63 - column 4, line 9, figure 3, claims 1-31, abstract	1,3,4
	--	
A	US 5757919 A (HOWARD C. HERBERT ET AL), 26 May 1998 (26.05.98), column 1, line 58 - column 2, line 5; column 6, line 31 - column 7, line 22, figures 5a,b, claims 1-24, abstract	1,3,4
	--	

INTERNATIONAL SEARCH REPORT

Information on patent family members

08/05/00

International application No.
PCT/FI 00/00421

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0798673 A1	01/10/97	AU 712353 B	04/11/99
		AU 2506297 A	22/10/97
		CA 2245921 A	09/10/97
		CN 1215489 A	28/04/99
		CZ 9802956 A	17/02/99
		EP 0960404 A	01/12/99
		JP 11506560 T	08/06/99
		NO 984535 A	28/09/98
		NZ 331258 A	28/10/99
		WO 9737331 A	09/10/97
US 5475763 A	12/12/95	NONE	
WO 9421066 A1	15/09/94	AU 683646 B	20/11/97
		AU 6255694 A	26/09/94
US 5369707 A	29/11/94	CA 2101198 A	28/07/94
US 5239294 A	24/08/93	AU 6034790 A	06/02/91
		CA 2063447 A,C	13/01/91
		IL 94467 A	31/12/95
		JP 2684118 B	03/12/97
		JP 5503816 T	17/06/93
		MX 166091 B	17/12/92
		WO 9101067 A	24/01/91
		CA 2087433 A,C	17/01/92
		JP 2750638 B	13/05/98
		MX 9100231 A	28/02/92
		WO 9202103 A	06/02/92
		US 5572193 A	05/11/96
US 5592553 A	07/01/97	EP 0636963 A	01/02/95
		JP 7107086 A	21/04/95
		US 5661807 A	26/08/97
US 5757919 A	26/05/98	AU 5688998 A	03/07/98
		DE 19782169 T	28/10/99
		GB 2334866 A	01/09/99
		GB 9912947 D	00/00/00
		WO 9826535 A	18/06/98